Testimony of Lawrence J. Zmuda
Partner, Homeland Security
Unisys U.S. Federal Government Group

Before the House Subcommittee on Economic Security,
Infrastructure Protection and Cybersecurity

November 4, 2005
Washington, D.C.

The Role of the Private Sector in the Rollout of the Registered Traveler Program

Chairman Lungren and distinguished members of the subcommittee, thank you for the opportunity to testify today before this subcommittee about the role of the private sector in the Registered Traveler program. My name is Larry Zmuda and I am a partner at Unisys U.S. Federal Government Group. I am proud to have led Unisys in its participation in three of the five TSA-sponsored Registered Traveler pilots.

Unisys supports many of the initiatives that are critical to securing this nation in the post-Sept.11 era. We have worked on securing cargo entering the country, identifying non-visa immigrants as they leave the country in the US-VISIT program, and, via the Registered Traveler program, have helped frequent travelers gain an expedited and predictable experience as they proceed through the security checkpoint. Because of Unisys participation in these programs, we understand and appreciate the balance required to ensure secure travel within our borders without impeding commerce.

In the spring of 2004, TSA competitively awarded to Unisys the contract for the Registered Traveler program. Five days after award, we began enrolling travelers.

We worked with Northwest Airlines in Minneapolis/St. Paul, United Airlines in Los Angeles, and Continental Airlines in Houston. We saw first hand how the airlines embraced this program and, more importantly, how the traveling public willingly provided biographical information and biometric data - their fingerprints and an iris scan - to expedite their security checkpoint experience. During the operation of these pilots, Unisys was in a unique position to understand the technology and its impact on the various stakeholders: TSA, the airports, the airlines, and, most importantly, the traveling public.

We were overwhelmed by the number of travelers voluntarily lining up to register for this program. In Minneapolis, we enrolled almost 2,500 people in one week and had

demand for more. For the pilots, though, TSA placed a cap on enrollments. All of the pilots, including the one in Orlando, have an enrollment limit. Notwithstanding this limit, the pilots that Unisys led provided some valuable metrics that validated this program. Enrollment and verification were quick and efficient. Travelers enrolled in less than 10 minutes and wait time at checkpoints could be calculated in seconds rather than minutes.

The pilots also showed how dual biometrics – in this case, fingerprints and iris scans - were critical in providing this service. Success rates were greater than 99 percent when dual biometrics were employed for identification. Additionally, the pilots tested smart card technology. Smart cards enhance security and capacity of the system. They're also more cost-effective in a nationwide program.

The demand to continue and expand this program is unmistakable. Initial feedback from participants in these first pilot programs was consistent. "When are you going to expand this to other airports around the country?" was the common cry in e-mails and discussions we had with them. In addition to the traveling public, the airport community has been equally enthusiastic.

To date, more than 50 airports have pledged their support to the Registered Traveler Interoperability Consortium (RTIC) that Mr. Barclay and the AAAE are spearheading. The airports see the benefits their customers are receiving and realize it is another way to improve their business.

The benefits extend not only to the participating airports, but to the economy as well as the traveling public for faster security processing. Once they've moved quickly through the security checkpoint, the travelers have more time to do work, shop at the stores, dine in the restaurants. This economic trickle-down effect is beneficial for local and national economies.

From a security perspective, improved process flow at the airports not only lessens the burden of the traveler, but of TSA. Because the registered travelers are known quantities, screeners can concentrate more attention on those travelers not known to them.

However, the airports and the TSA cannot perform all the requirements necessary to expand this program throughout the country. As with the five pilots, the private sector plays an important and critical role in the future of Registered Traveler to expand quickly and smartly across the nation.

Companies such as Unisys must be the driving force in the following areas:

- Capital investment
- Technology development
- Subject matter expertise
- Data privacy assurance

Financing for this program ultimately will come from those deriving the benefit, the traveling public. However, prior to taking a single fingerprint or iris scan and, therefore, one fee payment, significant capital investments must be made. All of the features of the program must be ready on day one. The solution must be built, tested and deployed. It is important to note that TSA always envisioned that Registered Traveler would be fully funded by fees and, therefore, not dependent upon Congress for funding.

The personnel who will enroll and aid the travelers at the checkpoints must be trained and paid. Work with communications and marketing firms regarding ways to reach the potential customers must begin. The business and operational processes must be in place to ensure smooth operations. All of these components combine to give people confidence that this is a program that will provide benefits without compromising security.

Several millions of investment dollars per airport are required to provide these capabilities. This is where the private sector can participate. Companies like Unisys understand all of the fiscal components and potential risks to smartly provide the capital investment required to launch this program. These are areas of expertise resident in the private sector; the government shouldn't be required to execute marketing or provide the latest biometric technologies. The federal government must devote its limited resources to providing security for all transportation modes.

Registered Traveler must allow multiple companies to participate. Competition will bring the best solutions and programs to the public. But competition must not bring with it solutions that do not work together. The technology that is developed and deployed at one airport must be interoperable with other Registered Traveler systems at other airports. This is the way to create a nationwide system.

The true benefit to the traveling public is interoperability – being able to use a card in airports across the country. Just as one can use ATMs at competitor's banks, the same must be true with airports. A registered traveler card issued by company X at airport Y must be able to work at another airport. The private sector must determine these standards and make them uniform – and public - so that all can benefit.

The private sector has an abundant supply of subject matter experts who can assist in determining standards that will streamline today's capabilities and that also will examine and predicts the future of the program. We must ensure that the technology is scalable and built in an open framework to handle the increasing volume should the program grow to the potential we are all anticipating.

This open architecture must be flexible enough to mesh with other federal programs and DHS initiatives, such as U.S.-VISIT, and potentially international programs looking to integrate with the United States. It would be untenable for programs not be interoperable after millions of dollars have been invested in them. Further, the technology must be accepting of new technology vendors as they enter the market.

With many of the patents iris vendors hold about to expire,, this could be critical in enabling all providers capable of participating in the program.

The private sector also can be the test bed for the latest technology. The program presently utilizes fingerprints and iris scans as the biometric verifiers. Technology must constantly stay ahead of the game to ensure the program remains secure. Radio frequency identification – RFID - capability and facial recognition are just two technologies that are gaining acceptance and could play a major role in near-future verification. The expertise resident in the private sector would help minimize risks associated with deploying new technology in a program that revolves around security.

Finally, the public is very concerned about providing sensitive personal data. Supporting that concern are an untold number of database hacking instances over the past year. The private sector must not and cannot own the data of those enrolling in the program, but we must ensure that it is safe and secure while it is in our possession. Every component of the solution that can accept personal data such as credit card numbers and addresses must be thoroughly secure. As the data necessary to perform the background checks is transmitted to TSA, encryption must be employed to prevent outside parties from gaining access to and tampering with the data. No one - neither the government nor the private sector - wants to be part of the public outcry that would ensue from such a situation.

My hope is that TSA embraces this opportunity to work with the private sector. TSA, along with Congress, must always weigh in should passenger security or privacy be compromised. In a competitive environment, companies like Unisys can facilitate the expansion of a Registered Traveler program, bringing the best solutions and utilizing the most effective technology in the most cost-efficient manner.

Thank you again for the opportunity to testify before you today. Unisys looks forward to assisting government agencies and lawmakers as they continue down a path where security is at the forefront of many of its decisions. I am happy to answer any questions you might have.